2013年10月11日星期五

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

华为油气企业信息安全解决方案

Author/ ID: 刘晨曦/90004552
Dept: 企业网络解决方案部
Version: V1.0(20130326)

enterprise.huawei.com
HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Content

由“铁人照片泄密”想到的。。。

他山之石——全球大企业信息化趋势

终端智能化

办公移动化

•2011年，智能手机出货量**4.7亿**部首次超过PC
•2013年，移动办公人员占比将达**35%**

IDC 2009-2015移动办公预测

大数据

4V

Volume 大数据量
Variety 多样性
Velocity 快速增长
Value 高价值

信息安全

“无边界”网络

办公网络界限模糊
公司、地铁、咖啡馆、机场、家

社交网络高速发展
企业重要的营销手段

云计算

企业部署私有云的百分比
2010，**35%**
2011，**+30%**

大企业中数据中心虚拟化的比例
2011，**59%**
2012，**65%**

HUAWEI

他山之石——全球大企业信息安全事故回放

2012年企业信息安全事件层出不穷

2012

SONY
索尼游戏用户个人信息(包括姓名、地址、登录密码等)被窃取，受影响用户约7800万，索尼信誉度严重受损，直接经济损失1.71亿美元。

FOXCONN The Art of More
黑客组织入侵了富士康的服务器，获得代工客户姓名和密码(可以伪造苹果、微软等公司订单)，同时富士康所有邮件账户和密码被公开，其中包括CEO郭台铭。

NEUSOFT 东软
东软集团副总经理伙同研发核心人员窃取医用CT机核心技术自立门户研发生产CT机，涉案人员28人，案值6400多万元。

vmware
VMware的ESX Hypervisor的源代码被黑客公布在互联网上，Vmware不得不建议用户马上升级到最新代号为ESXi的hypervisor。

HYBROTHERS 华谊兄弟传媒
华谊兄弟网络被黑客入侵，黑客获取了登录证书并在互联网上公布入侵情况。

企业因信息安全事件损失惨重

- 2011年，全球共计登记信息泄露事件819起，总损失金额超过**200亿**美元
- 网络攻击给全球带来了**1110亿**美元的损失
- 在Fortune排名1000的公司中，每次电子文档泄密造成的损失平均为**50万**美元
- 据国安部统计，我国63.6%的企业用户处于“高度风险”级别，每年因网络泄密导致的经济损失高达上**百亿**。

HUAWEI

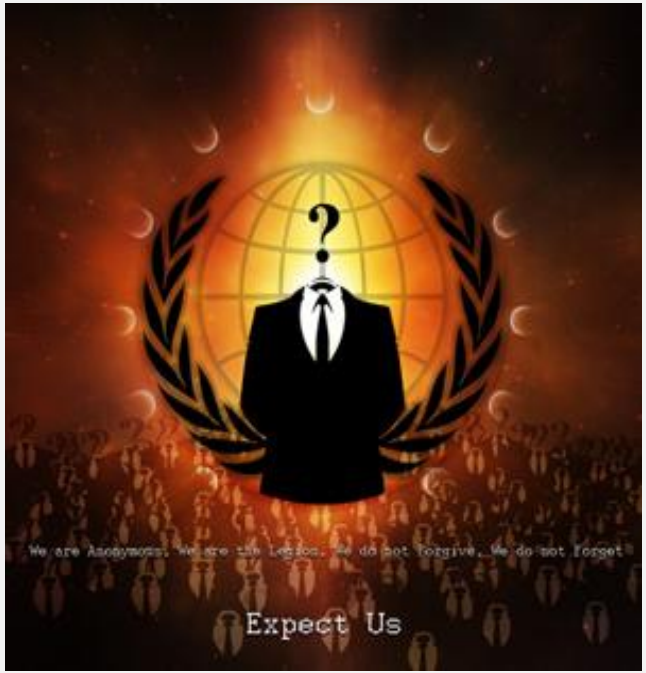
全球大型油气公司面临黑客安全威胁

黑客组织Anonymous威胁中石油等全球石油企业

•2012年11月，著名黑客组织Anonymous宣称由于油价上涨等因素，要对包括中石油、中石化在内的全球25家大型石油企业发动代号为“OpFuelStrike”的网络攻击。

•Anonymous是一个攻击水平很高的黑客组织，具有较高的命中率，因此相关企业的安全风险大幅提升，这次代号为“OpFuelStrike”的攻击声明非常值得石油企业保持高度警惕。

•Anonymous还先后组织过针对Sony、万事达、中情局（联手维基解密）等知名机构的攻击，在社会上影响较大。



我们是Anonymous
我们是军团
我们不会原谅
我们不会忘记

信息安全给油气企业信息化带来的挑战

安全管理

◆ 油气企业组网复杂，网络设备多，安全事件独立，无法端到端分析安全事件

◆ 当安全事件发生时，如何快速定位解决并分析回溯

◆ 安全策略如何集中快速部署

内部泄密

◆ 油田勘探数据、市场运作、财务数据、公司策略等机密资料属于高价值资产

◆ 内部员工可能会将机密信息转移出去，销售给竞争对手

◆ 泄密手段多样化，如终端拷贝、打印，邮件、web网络等

恶意攻击

◆ 攻击终端：通过网络攻击在终端置入木马，窃取机密信息

◆ 攻击服务器：通过攻击服务器获取权限，窃取信息数据

◆ 攻击网络和服务：造成网络不畅，甚至网络瘫痪

IT特权滥用

◆ IT运维人员可以接触公司的各种机密数据，泄密更容易

◆ 企业管理人员IT特权滥用，导致机密资料有意或无意泄露

HUAWEI

先解剖一个麻雀——助力中国商飞构建完整信息安全体系

挑战

•中国商飞作为涉密单位及高新技术企业，信息安全**面临极大的压力**，尤其是对网络的**安全状况无法感知**

•快速整合众多单位，安全意识和安全状况**参差不齐**，安全设备多样化，**无法有效管理**

•请国内一家安全公司做过安全咨询服务，但该公司没有信息安全建设经验，安全制度、安全策略**无法真正的落地**

解决方案

•以华为信息安全最佳实践为参考，通过安全咨询服务，构筑**完整的**信息安全体系

•识别关键问题，**分阶段实施**

•优先提升**防泄密**能力、**安全运维**能力、**全员安全意识**

HUAWEI

Content

华为信息安全建设成果

- 防病毒平均每月阻断病毒击 **55万次**
- 平均每月阻断网络威胁 **49.2万次**
- 阻断SQL注入/跨站攻击等 **300万次/年**
- 所有DDOS攻击的阻断

- 文档加密授权：黑客等非法窃取后，数据无法阅读
- 硬盘介质加密，防止丢失后数据泄密
- 2006年至今，发现一级泄密事件**56次**，其他级别**141次**

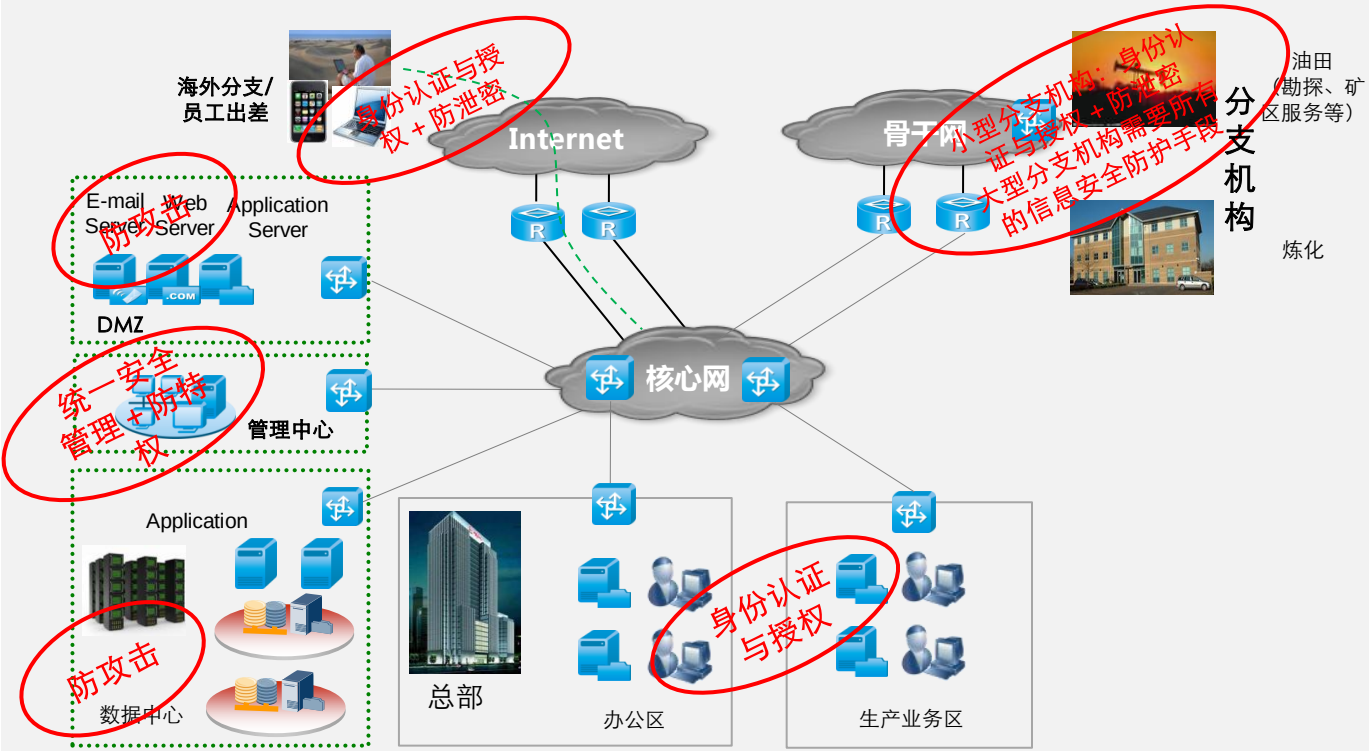
- WSUS升级率为一周 **80%**
- 防病毒四小时内整体更新率超**90%**
- 有效防止IT特权滥用

- 管理者效率提升**9.4%**
- 业务代表效率提升**12.5%**
- 办公安全高枕无忧；

HUAWEI

油气企业信息安全方案框架

油气企业整网信息安全防护



业务/网络特点：

- 横跨地域广阔，业务系统与信息数据跨地域传输；
- 承载油气企业办公，生产等多样的业务应用；
- 核心业务与数据集中在总部数据中心
- 组网方式灵活，采用无线，微波，光纤等，纵向/横向多区域的组网架构；
- 内部人员复杂，除了办公人员外，还需要为员工家属提供网络业务承载；
- 网络规范庞大，管理复杂，运维成本高；

HUAWEI

防泄密

防泄密

关键信息识别

- 关键信息资产识别
- 关键信息资产定称密级
- 指定信息资产保护策略

信息资产安全管理

- 核心信息统一管控
- 关键文档集中授权

网络数据安全防护

- 业务数据分区保护
- 关键数据外发管控
- 远程数据保密传输

终端信息安全管控

- 终端数据安全管控
- BYOD终端防泄密

泄密事件审计追溯

- 数据访问审计
- 邮件外发信息审计
- 上网行为审计
- 终端行为审计

HUAWEI

油气企业信息资产安全管理

- 集中管理
- 安全管控
- 查阅管控
- 加密管控
- 追踪管控

- **集中管理，避免信息流失**
  - 多业务多来源信息数据集中存管
  - 汇集信息便于查阅检索
- **安全管理，保证信息安全**
  - 统一设置数据安全级别
  - 查阅、加密、打印、追踪等不同管控手段
- **个人空间备份，提供在线编辑**
  - 个人空间存储服务，防止数据丢失
  - 多格式在线编辑和播放，防止内部人员泄密

建立信息中心，提供加密、审计等管控手段，协助用户安全管控信息资产

HUAWEI

三大手段保障油气企业数据传输安全

远程数据保密传输

通过运营商或专网部署企业VPN（油田、炼化、分公司）

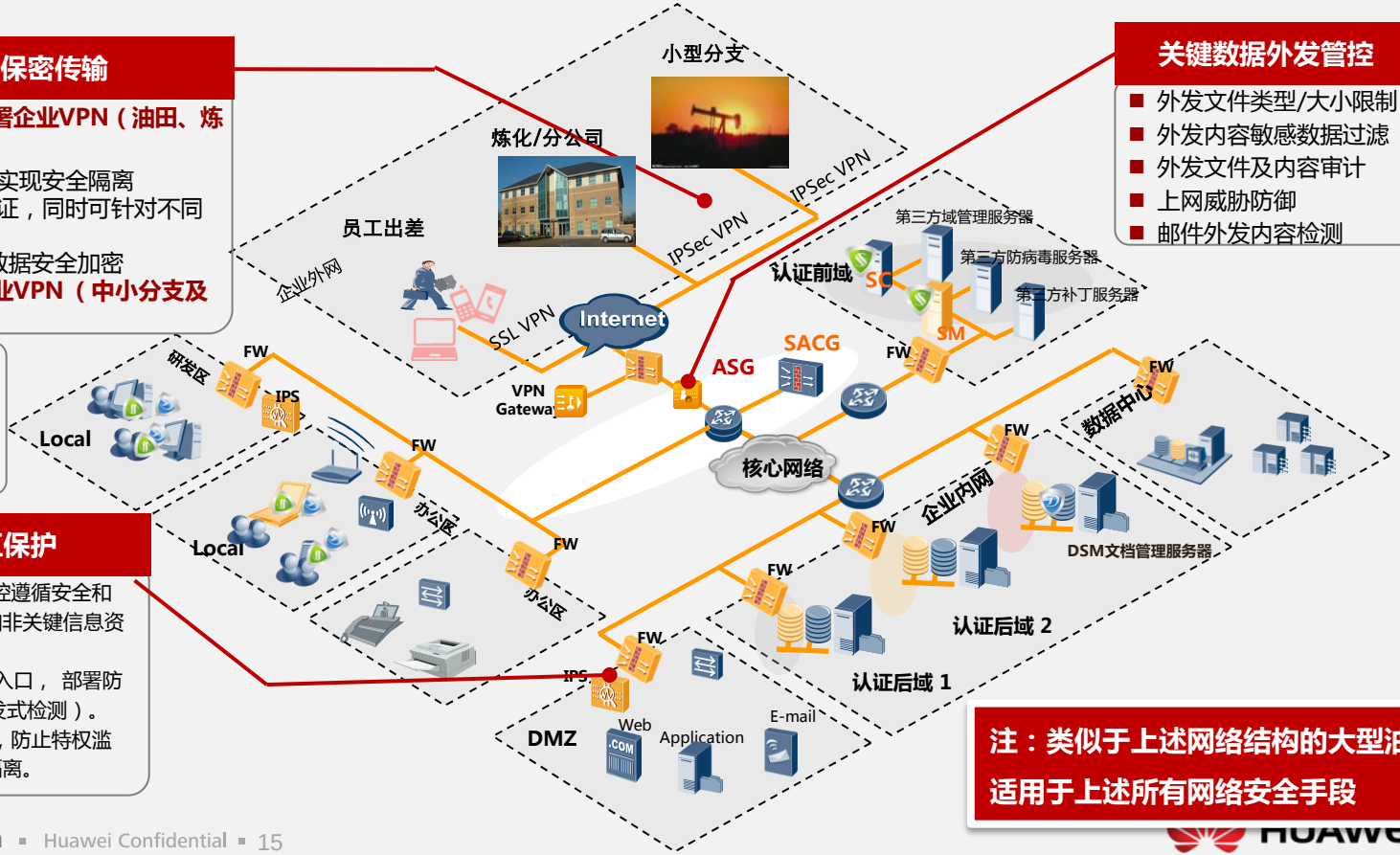
- 对企业的不同业务实现安全隔离
- 企业业务高质量保证，同时可针对不同的业务作不同的QOS;
- IPSec为分支提供数据安全加密

通过internet部署企业VPN（中小分支及移动用户接入）

- IPSec为办事处提供数据安全加密
- SSL VPN为个人用户提供接入认证和数据加密;

业务数据分区保护

- 安全区的划分和访问管控遵循安全和效率均衡原则（区分关键和非关键信息资产）。
- DMZ/Externet/研发区入口， 部署防火墙+IPS（基于漏洞、启发式检测）。
- 运营管理区部署堡垒机，防止特权滥用其余区域间部署防火墙隔离。

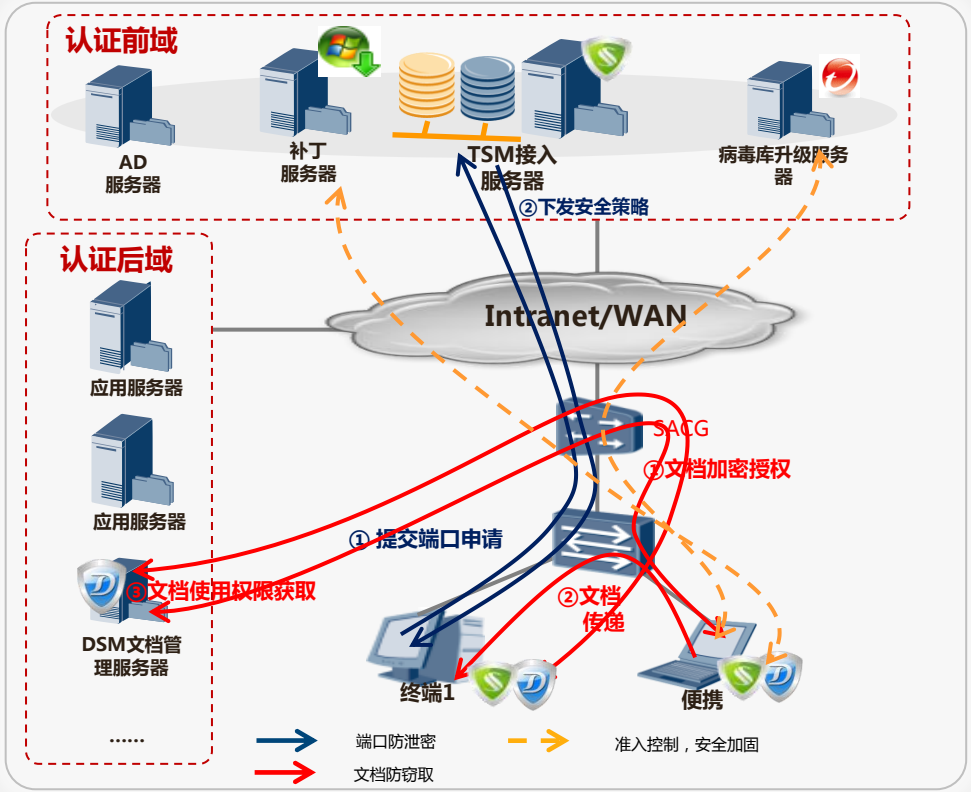


关键数据外发管控

- 外发文件类型/大小限制
- 外发内容敏感数据过滤
- 外发文件及内容审计
- 上网威胁防御
- 邮件外发内容检测

注：类似于上述网络结构的大型油田适用于上述所有网络安全手段

终端数据安全：端口管理+文档加密+漏洞修复



介质防泄密，文档防窃取

终端全生命周期安全防护

安装 → 使用 → 退库

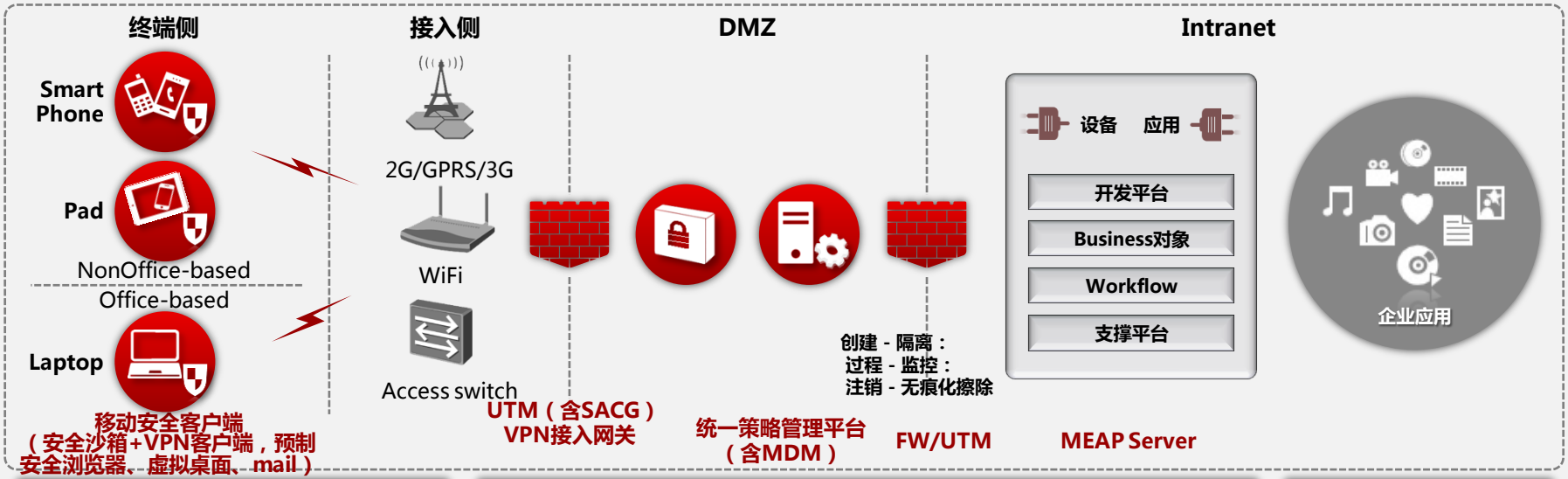
- 端口使用申请监控
- 制定USB加密策略，控制数据交换
- 移动介质申请使用
- 文档加密授权
- 便携硬盘加密
- 禁用端口
- 便携回收，硬盘低格或销毁
- 移动介质回收格式化

准入控制，安全加固

- 终端漏洞一键式修复(漏洞扫描，补丁、病毒库升级)

HUAWEI

BYOD终端防泄密



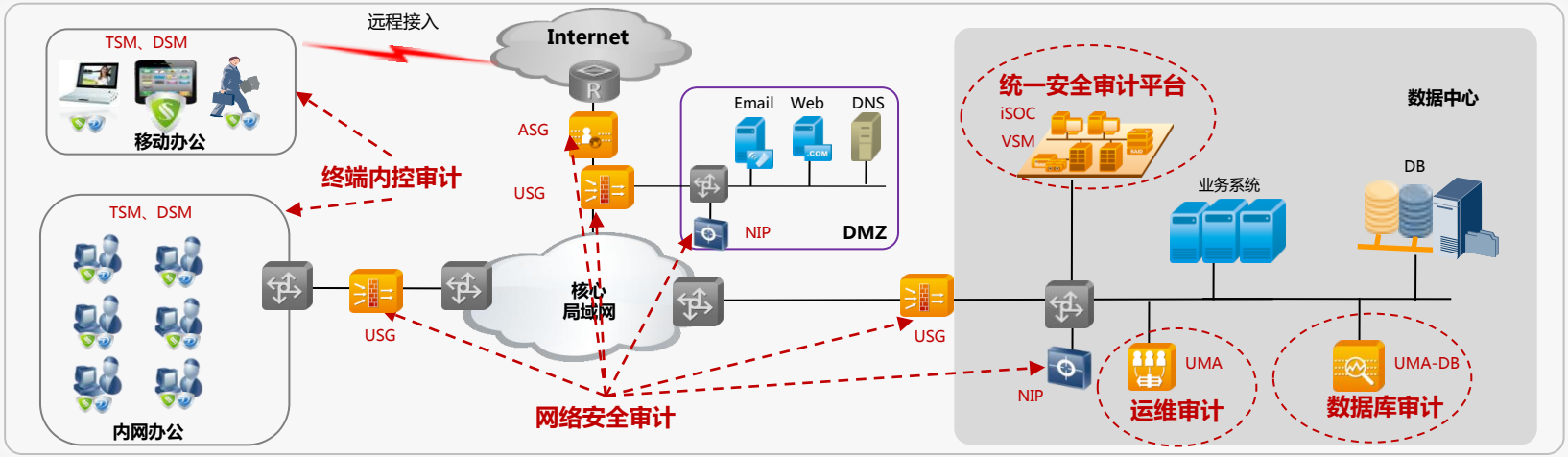
身份 Identity		隐私 Privacy				遵从 Compliance	
认证授权	接入控制	链路安全	威胁防护	数据保护	应用安全	管理安全	
• 移动强认证	• 移动NAC	• SSL/UDP隧道加密 • Web VPN • L3 VPN	• DDoS • 网络AV • 网络IDS/IPS	• 移动沙箱 • Web/Email DLP • 反盗窃	• 应用监控	• 安全管理 • 应用管理	• 资产管理 • IT服务

- 可应用于**生产网移动巡检、办公网移动OA/移动ERP**等场景

- **E2E解决方案能力强**
- **移动终端安全能力强**

HUAWEI

泄密事件审计，全网追踪溯源



终端内控审计	网络安全审计	数据库审计	运维审计	统一安全审计平台
•终端用户行为审计 •操作系统和服务审计 •文档操作审计 •存储介质使用审计 •终端软硬件资产管理	•网络流量会话日志 •应用漏洞检测审计 •员工上网行为审计 •邮件审计 •网络安全事件日志	•细粒度数据库会话审计 •数据库操作过程记录 •支持各主流数据库平台	•系统管理员和维护人员对核心业务系统的操作行为审计 •支持各主流运维方式	•全网日志集中管理 •全网安全事件集中管理 •关联分析，预警通知 •报表、报告输出

HUAWEI

防攻击

防攻击——深度检测，全面防护

攻击防护

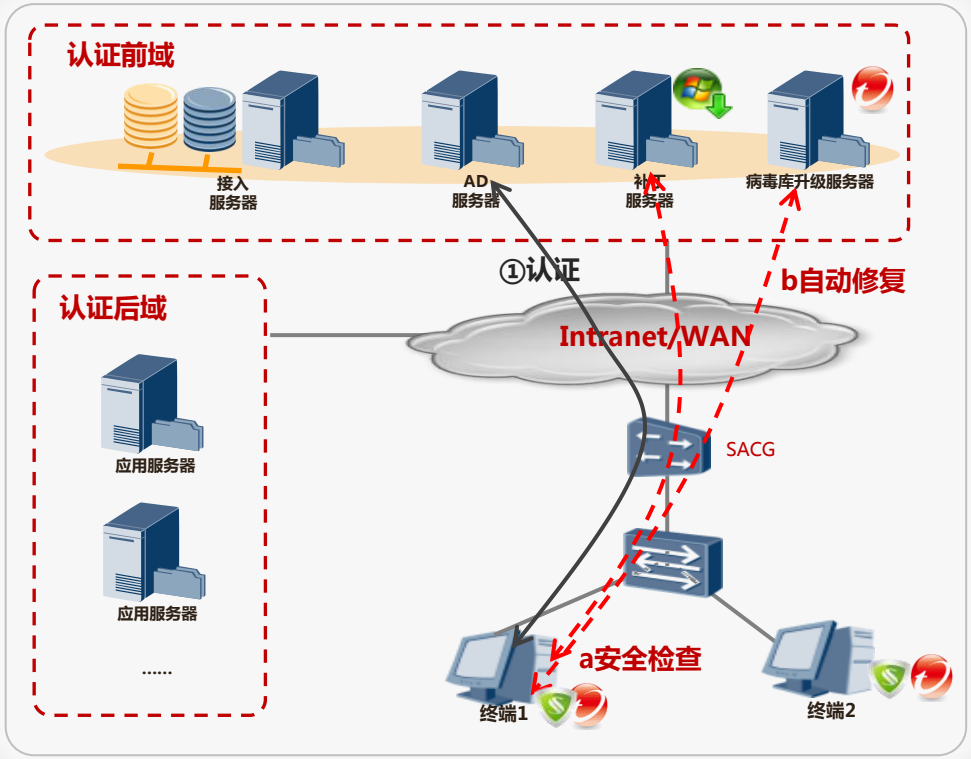
终端安全防护
- 终端准入控制、安全加固

网络安全防护
- 攻击入侵深层检测，全面防护
- 高性能、易管理

服务器防护
- 网络防护+攻击预警+主机保护+漏洞管理

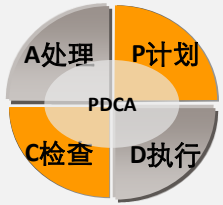
应用安全防护
- WEB防攻击
- Email全面保护

终端防攻击——准入控制，安全加固



终端准入控制

- 定制终端接入策略
- 阻止非法终端用户接入
- 隔离修复不合规终端用户
- 授权终端用户访问资源
- 监控终端用户行为便于审计取证



终端安全加固

补丁、漏洞、病毒库一键式修复、更新

安全检查

- 登陆密码复杂度是否合规
- 检查软件黑白名单
- 检查可疑注册项
- 检查防病毒软件
- 检查补丁
- .....

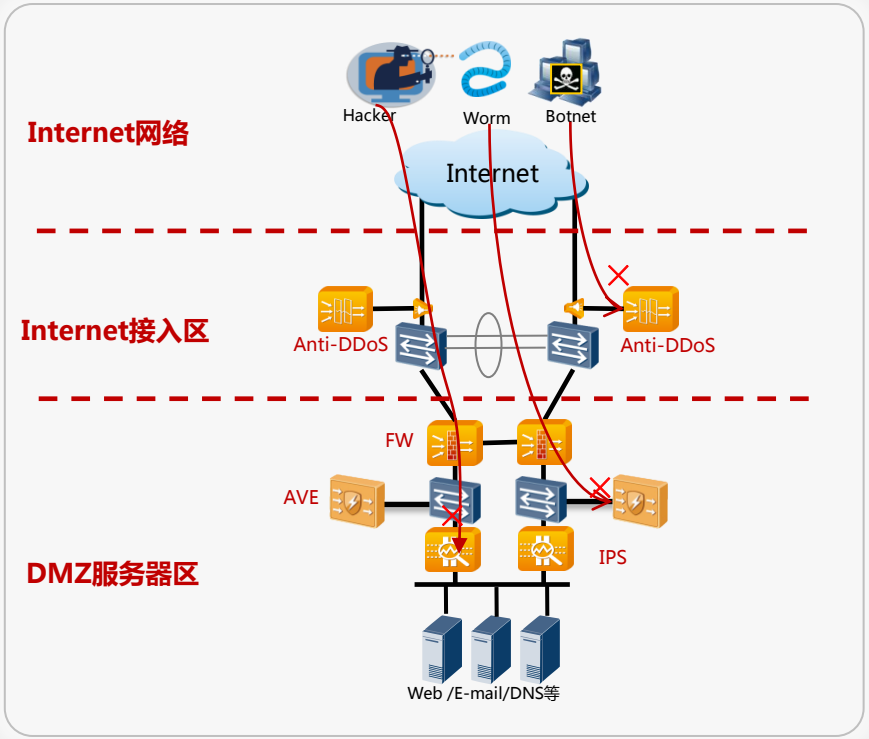
一键式自动修复

自动修复

- 按规范更改密码
- 安装了指定的应用软件
- 安装了正确版本的AV
- 病毒库已更新
- 安装了最新的OS补丁

HUAWEI

网络防攻击——深层防护、性能无忧



网络深层防护

- ◆基于DPI的七层DDoS防护
- ◆通过防火墙进行安全域划分，DMZ域隐蔽、访问控制
- ◆基于漏洞和启发式的入侵检测，对付新型/变种攻击
- ◆AVE 防病毒网关保证企业内网安全

网络高性能防护

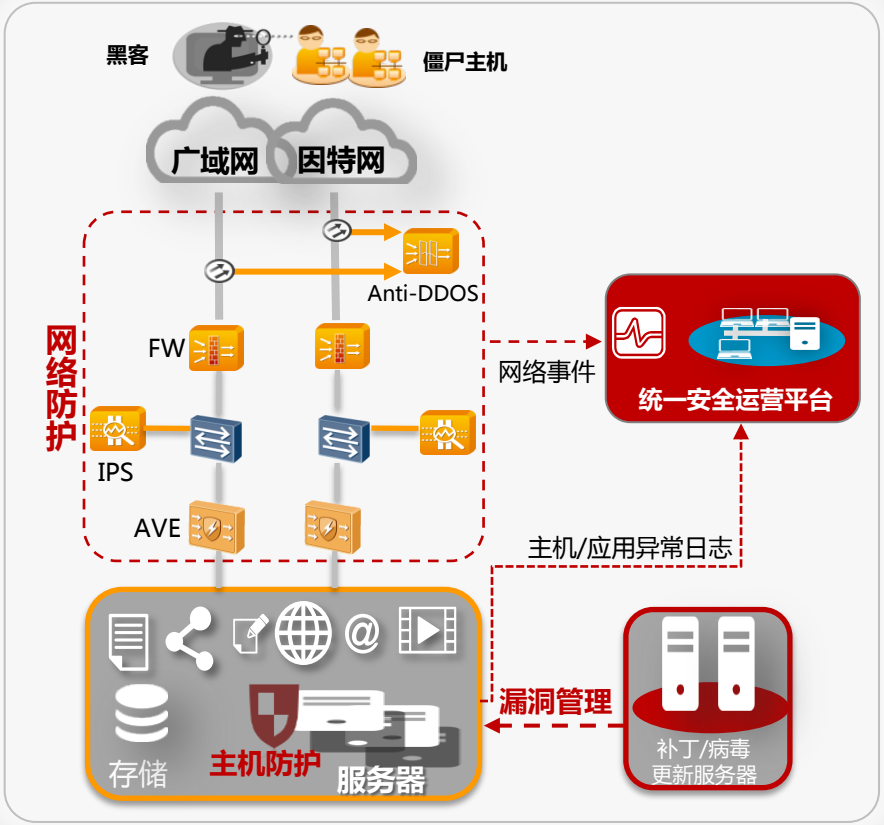
- ◆单台Anti-DDoS设备性能达160G，10000个IP地址精细化防护，100万个IP地址的普通防护
- ◆平均无故障时长50万小时，99.9999%可靠性
- ◆七层防御架构，全面防御应用层攻击和IPV6攻击
- ◆秒级检测、秒级清洗

易管理易扩容

- ◆分布部署，集中管理；差异化防御、丰富报表；灵活取证方式，方便审计
- ◆线性扩容，提高投资利用率，节约扩容成本

HUAWEI

四级安全防护，保障服务器稳定可靠



网络攻击保护：

防DDOS攻击+防火墙过滤+入侵检测+病毒防护

攻击分析预警：

主机行为日志 + 网络安全事件 + 攻击检测
=> 关联分析 => 发现攻击威胁 => 预警

主机防护：

主机防火墙：阻挡非法网络嗅探、避免越权访问
主机防病毒：避免病毒、恶意软件、危险邮件感染服务器
主机IPS：为服务器打上“虚拟补丁”

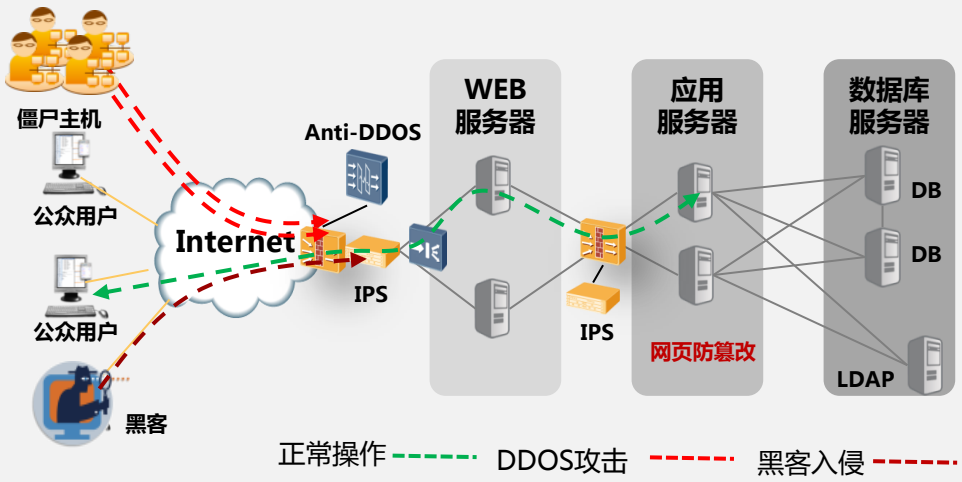
漏洞管理：

漏洞扫描
配置核查
补丁更新

四级防护，安全可靠

HUAWEI

应用防攻击——全面保护企业邮件系统及WEB应用



Web安全防御

- 对DDOS攻击流量清洗，保证正常访问
- 安全域划分，分层部署，层级访问控制
- 部署WAF，阻断黑客基于WEB系统漏洞攻击
- 部署网页防篡改系统，及时阻止和恢复被篡改的网页

Email全面防护

- 防垃圾邮件
- 防病毒
- 防攻击
- 防钓鱼
- 内容过滤

HUAWEI

防IT特权滥用

IT特权滥用挑战

维护入口多

- 众多维护入口，无法控制人员接入设备系统
- 运维设备系统众多，运维方式难统一

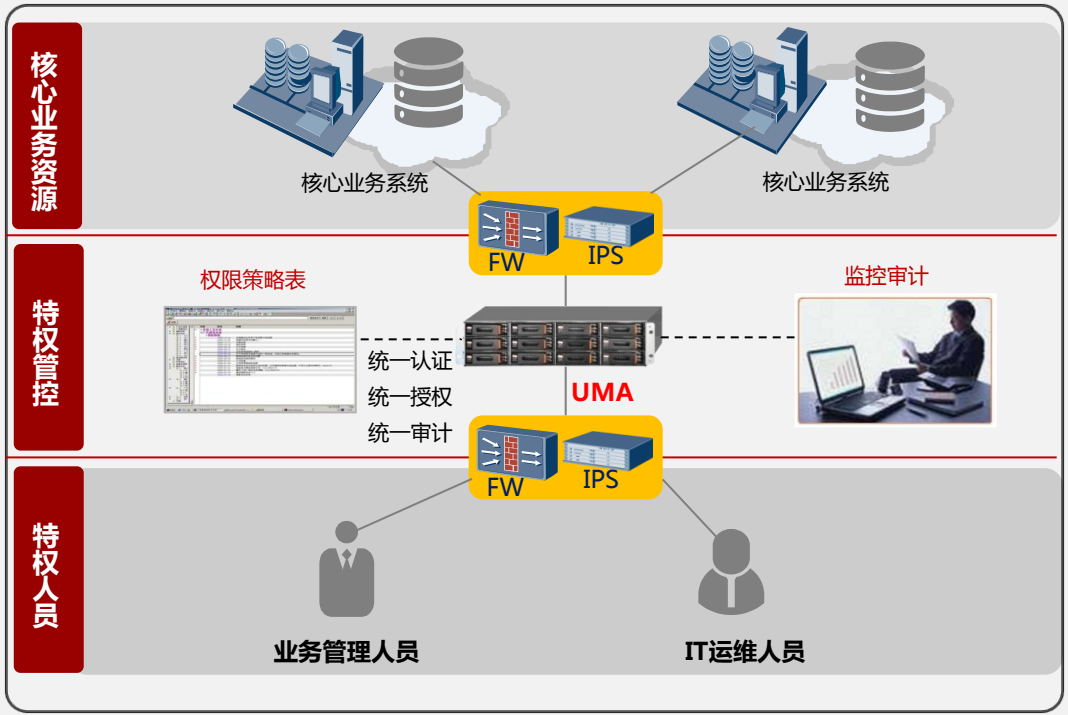
权限控制难

- 运维账号维护不及时，存在运维人员非法登陆风险
- 运维人员账号权限过大，误操作或越权操作影响系统运行

数据访问乱

- 运维人员运维过程非法访问核心数据，导致机密数据泄密
- 企业业务管理人员IT权限没有有效监控审核，存在机密信息泄露风险

防系统越权操作——统一运维入口，统一权限管理



- 统一运维入口，实现单点登录
- 账号集中管理，人与系统账号严格一一对应
- 权限严格控制，依据角色分配
- 特权滥用全面审计，准确回溯

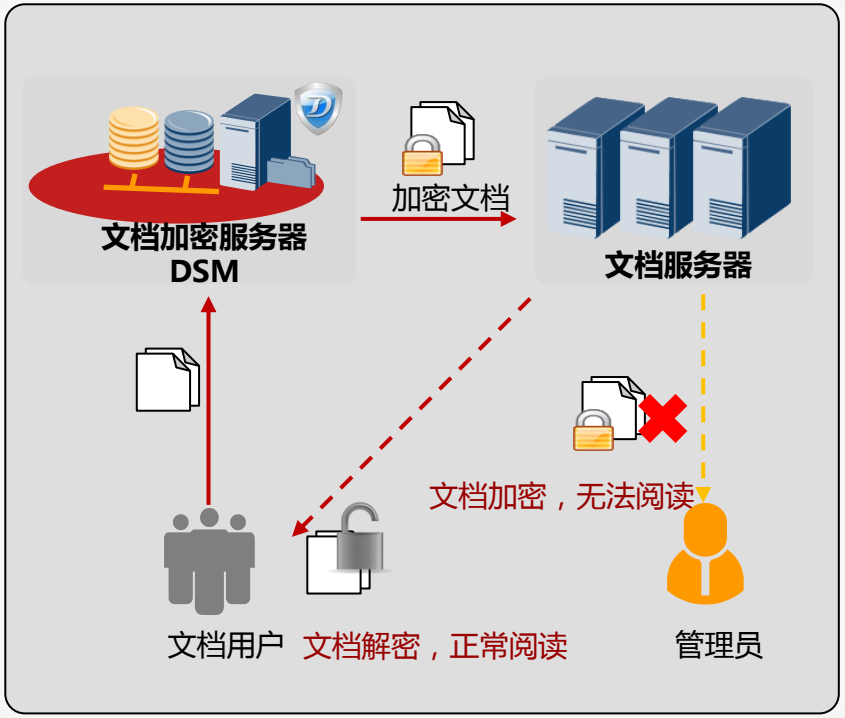
HUAWEI

防数据越权访问—虚拟机数据加密存储，防止非法访问

通过虚拟磁盘加密技术，将VM数据全部加密存储，防止管理员通过非法挂卷越权访问客户数据

HUAWEI

防数据越权访问—文档数据加密存储，防止非法访问



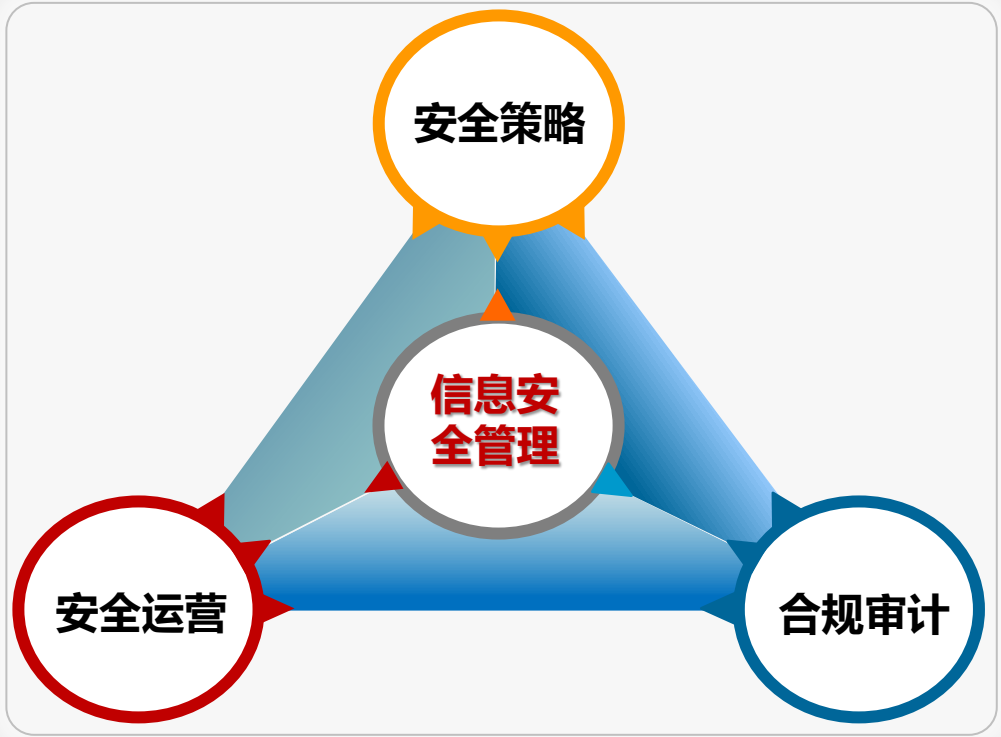
文档加密存储

✖ 通过DSM文档加密授权，防止文档服务器管理员非法访问

√ 文档用户将加密的文档下载到本，依据自身权限进行解密阅读

安全管理

信息安全管理



安全策略
- 可视操作化
- 安全策略集中配置
- 全网管理

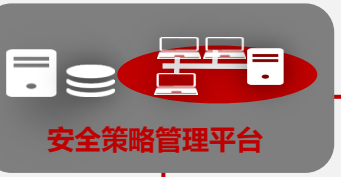
安全运营
- 安全事件管理
- 安全风险管理
- 统一运维
- 防IT特权

合规审计
- 数据库审计分析预警
- 满足合规遵从的强制要求（萨班斯法案，等级保护，ISO27002）

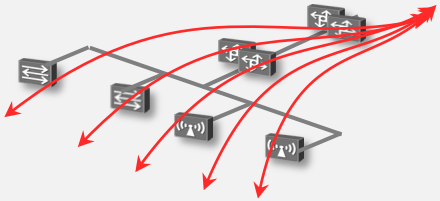
HUAWEI

安全策略管理平台让策略管理简单可靠

HUAWEI VSM



统一管理、深度管理



- 数通、安全统一管理
- 从网元管理深入到业务策略管理

可视业务运维、诊断专家

- 可视化策略管理和操作界面
- 面向业务的网络监控和测试诊断
- 快速故障定位和告警分析

快速集成、开放平台

- 提供多种北向接口
- 可扩展、增量式的扩容升级

安全策略集中配置，批量下发，操作简单，高效可靠

HUAWEI

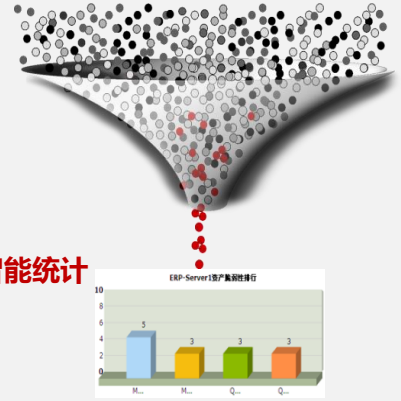
安全运营与合规审计，全面掌控企业安全运营

HUAWEI iSOC

统一安全运营平台

- 安全事件分析
- 安全风险预警
- 安全运维管理
- 合规审计管理

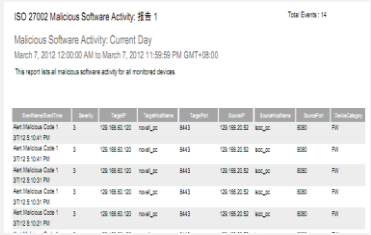
海量安全事件分析:
- 基于统计关联分析
- 基于资产关联分析
- 基于规则关联分析



安全风险及时预警，智能统计

统一安全运维管理:
- 统一核心业务系统入口
- 集中账号管理
- 权限严格控制(资源级别、命令级别)

合规审计:
- 记录操作过程，快速故障定位和责任分析
- 为第三方审计机构提供审计报表和原始日志

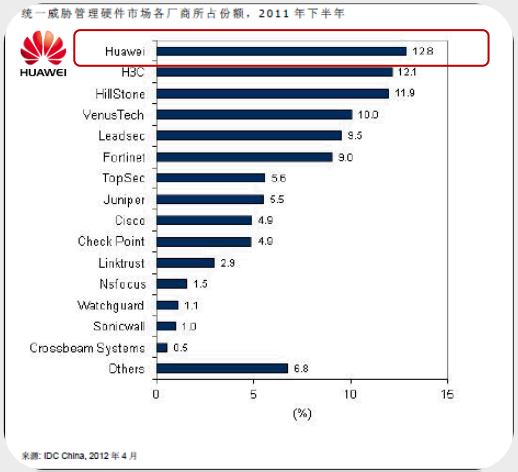


HUAWEI

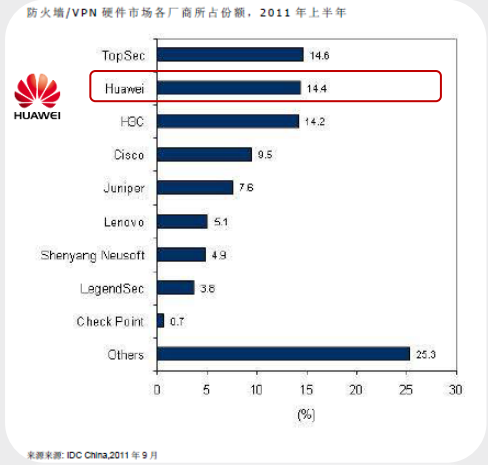
Content

华为安全在业界的认知度

IDC 2011 China



IDC 2011 China



国内市场份额领先

- 华为UTM产品，2011年中国市场份额 12.8% 排名第一
- 防火墙/VPN产品，2011年中国市场份额 14.4%排名第二

NSS Labs
"Very Good" @ 恶意软件检测

westcoast labs
Checkmark UTM 证书

ICSA labs
网络防火墙证书

IPv6 Ready
网络防火墙

全球多项资质认证

- 国际多项认证，实至名归

HUAWEI

华为安全能力

深度包检测

- 支持协议850+
- 主流应用协议全覆盖
- 支持热门加密P2P协议
- 快速响应定制化需求

Web 分类

- 已分类站点 >6500万
- 准确率 >96%
- 分类种类 >130种

Web 信誉

- 恶意URL检测>2000万
- 钓鱼网站检测>50,000,
- 准确率>90%

恶意插件防护

- 已识别僵尸网络: 350+
- 准备蠕虫识别：500+

病毒防护

- 病毒库: 150,00万 million
- 攻击签名识别：6500+

入侵防御

- 零日攻击智能识别
- 攻击签名识别: 20000+

华为安全产品总览

安全服务

能力中心

僵尸网络特征库	垃圾邮件库
应用协议分类库(DPI)	URL分类库
病毒/恶意代码特征库	入侵/漏洞特征库

服务中心

安全应急响应	安全管理中心
在线升级平台	安全管理服务
信誉评估中心	安全咨询

合规管控

iSOC统一安全管控 UMA统一运维审计OMM视频信息管控中心 OIC文件信息管控中心

安全管理

elog日志管理系统 VSM安全管理系统

应用安全

上网行为管理

ASG2100/2200 ASG2600/2800

业务智能网关

SIG1000E SIG9280E SIG9800-X3 SIG9800-X8 SIG9800-X16

DDoS防护网关

AMS1000 AMS8000

网络安全

安全接入网关

SVN2000 SVN5000

安全路由网关

USG2000/5000BSR

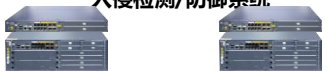
统一威胁管理

USG2000 USG5000

数据中心安全网关

USG9000

入侵检测/防御系统



NIP2000D/NIP5000D NIP2000/5000

终端安全

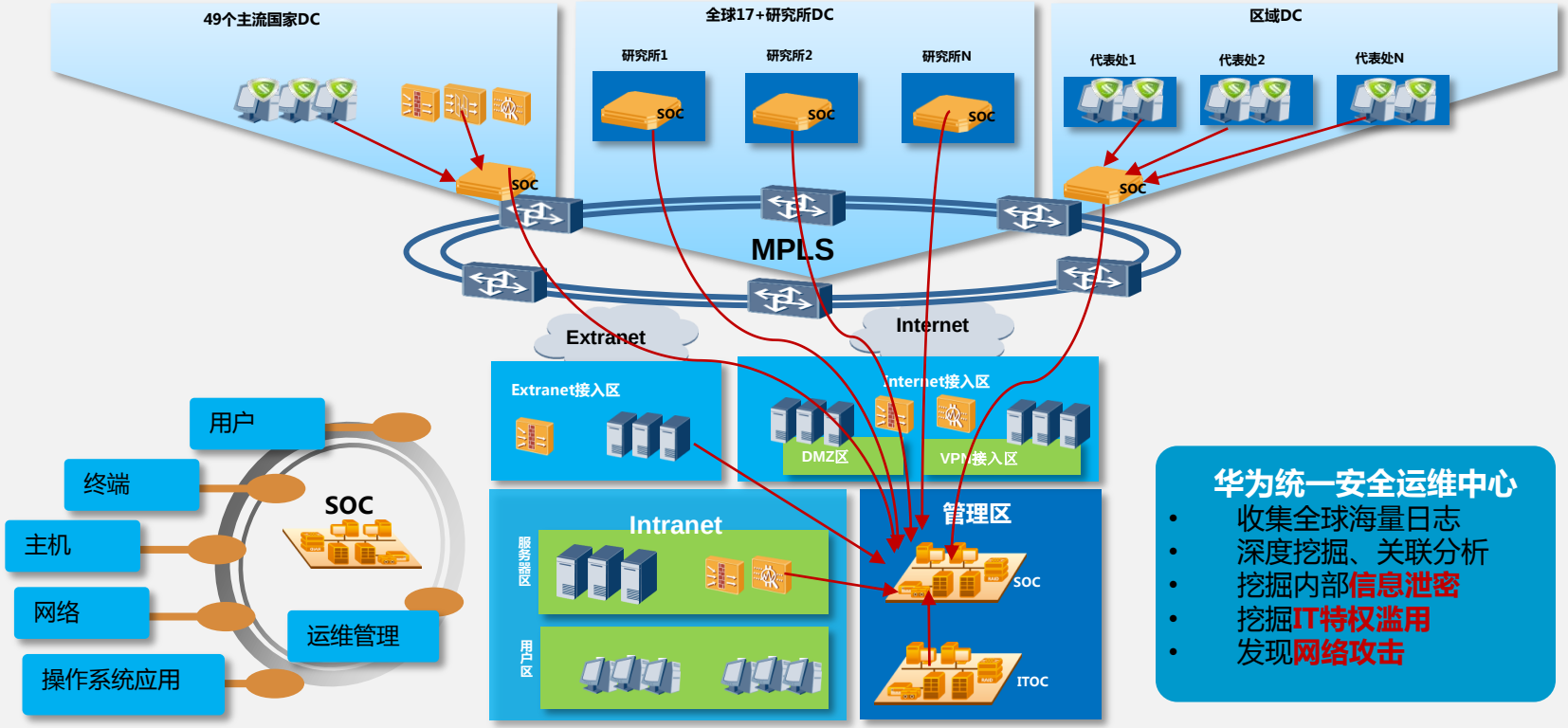
TSM终端安全管理

USG2200TSM安全一体机

DSM文档安全管理

Content

华为公司信息安全建设实例



华为统一安全运维中心

- 收集全球海量日志
- 深度挖掘、关联分析
- 挖掘内部**信息泄密**
- 挖掘**IT特权滥用**
- 发现**网络攻击**

HUAWEI

中石油加油站管理系统VPN项目

挑战：

中石油全国共有上万个加油站，网络建设方案的可实施性，可用性，可靠性以及经济性是中石油加油站管理系统建设过程中必须考虑和解决的问题。

加油站业务数据的安全性及设备的易用性也是整个方案关注的重点。

华为解决方案：

在全国加油站采用华为USG2110系列安全路由网关作接入网关，通过pppoe方式为边缘网络提供广域网接入，提供防火墙等功能；通过IPSec VPN隧道保障信息安全和服务质量。

各省中心采用USG2200系列安全路由网关，提供各省加油站IPSec VPN的汇聚以及业务数据的上联。

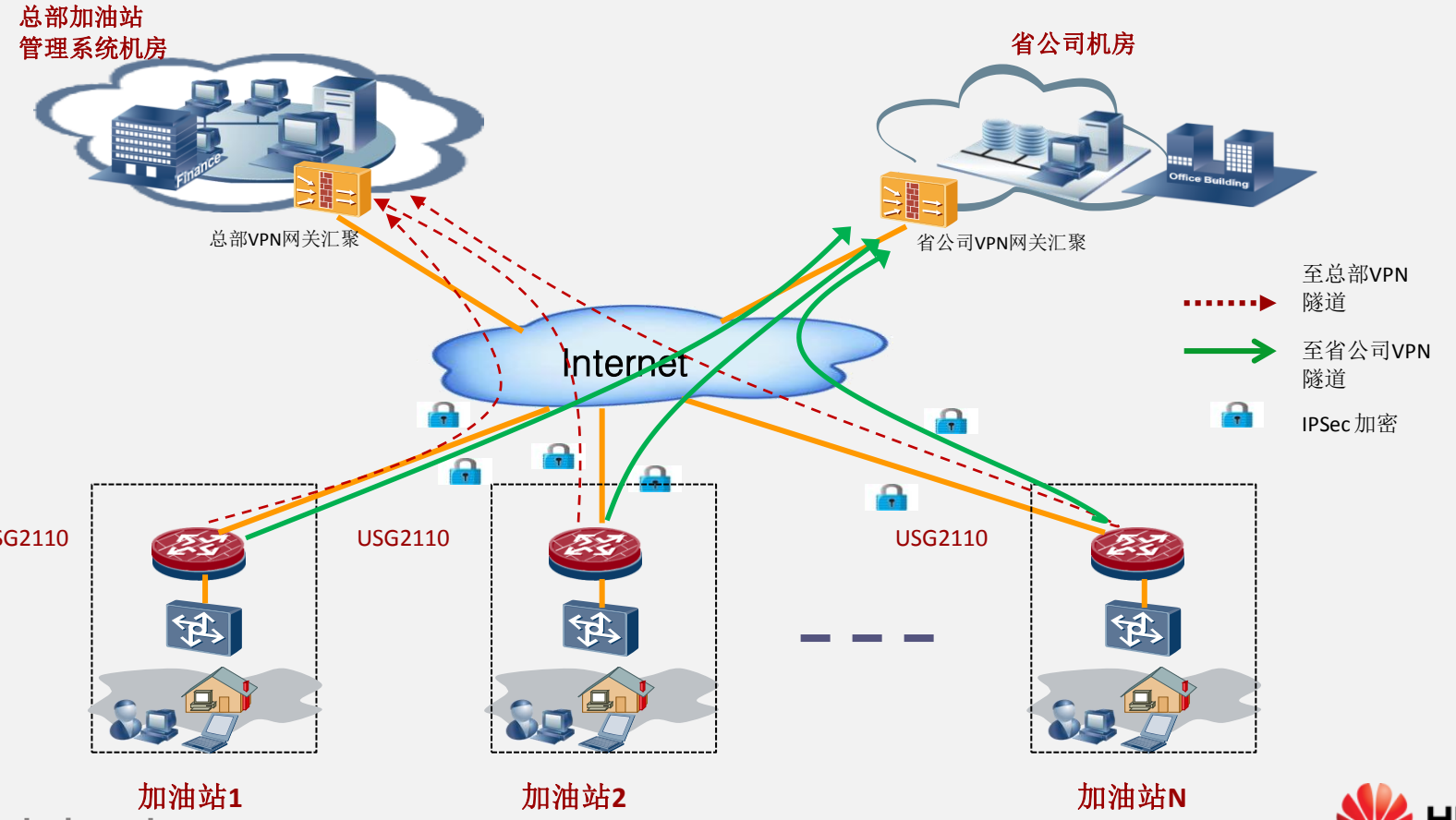
客户价值：

- ✓ 中石油加油站管理系统VPN网络项目，建设周期短，投资少，安装简单，维护方便；
- ✓ 路由、安全、VPN与一体的解决方案，充分保障了信息安全；
- ✓ 通过采用华为公司VPN解决方案及产品，进一步提高了企业的业务水平和信息化业务的应用质量。

中国石油天然气集团公司（简称中国石油集团）是一家集油气勘探开发、炼油化工、油品销售、油气储运、石油贸易、工程技术服务和石油装备制造于一体的综合性能源公司。在世界50家大石油公司中排名第5位。中石油在2008年世界500强公司排名中居第25位。

HUAWEI

中石油加油站管理系统VPN解决方案



HUAWEI

中石油广域网VPN接入项目

挑战：

中石油整个网络规模庞大，分支机构遍布国内外，VPN登录用户可能来自国内外不同的角落，相对分散。要使用户拥有更好的使用体验，同时保持方案的持续领先 确保系统的技术领先性和持续发展性。

华为解决方案：

针对不同机房、不同网络出口部署单独的VPN系统，同时多个系统之间互为备份；

VPN的部署使用集群负载均衡的方式，通过负载均衡和集群为用户智能优选登录节点，提高用户使用体验；

提供可靠高效的VPN服务并保障整个系统的可靠性；

集群设备可统一管理，也可分级管理，实现维护管理的灵活性和易用性；

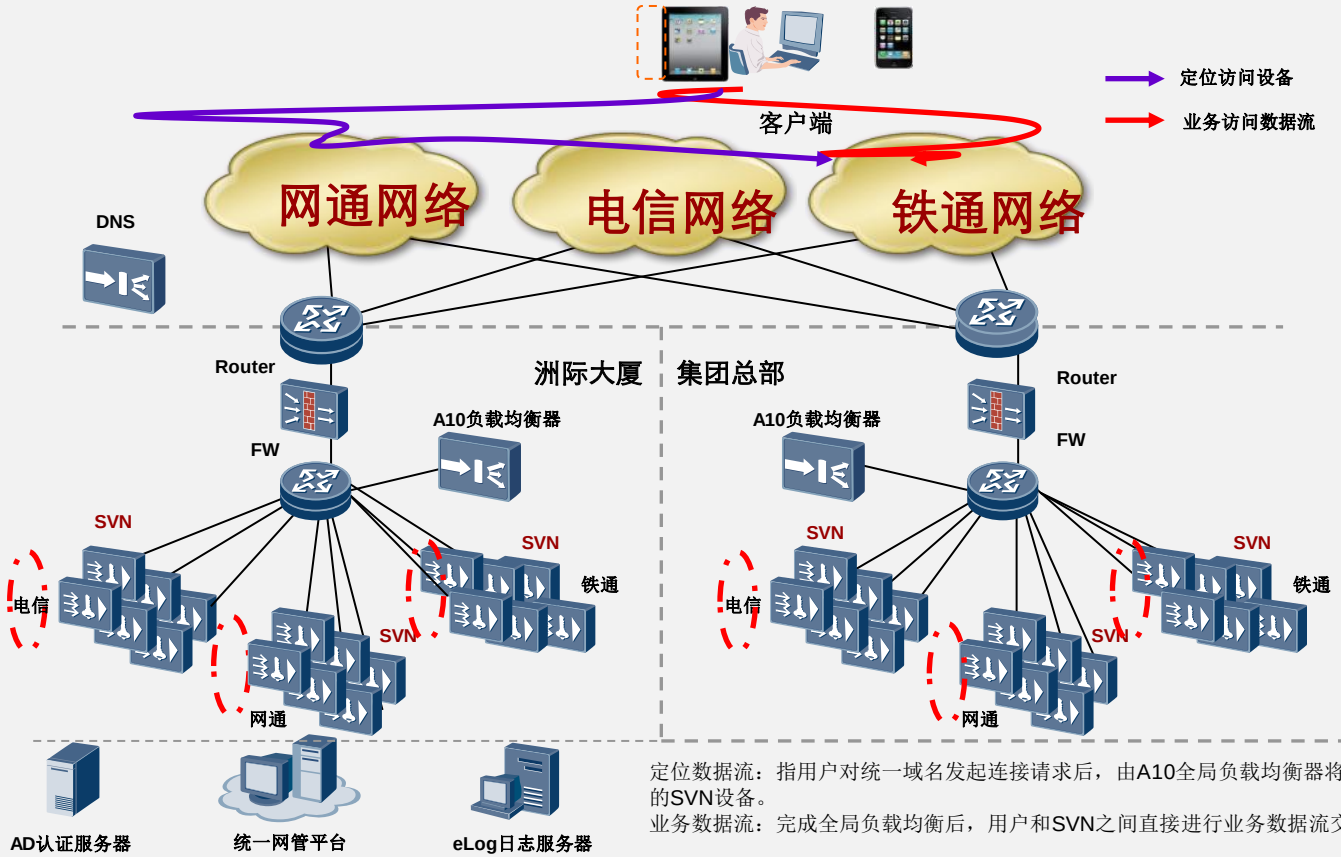
客户价值：

- VPN业务的高可靠性；
- 就近接入保证用户体验；
- 为遍布全球的分支机构、勘探队提供随时随地、安全可控的接入方式，有效提高工作效率，降低沟通成本；

中国石油天然气集团公司（简称中国石油集团）是一家集油气勘探开发、炼油化工、油品销售、油气储运、石油贸易、工程技术服务和石油装备制造于一体的综合性能源公司。在世界50家大石油公司中排名第5位。中石油在2008年世界500强公司排名中居第25位。

HUAWEI

中石油广域网VPN接入解决方案



定位数据流：指用户对统一域名发起连接请求后，由A10全局负载均衡器将用户访问重定向到具体的SVN设备。

业务数据流：完成全局负载均衡后，用户和SVN之间直接进行业务数据流交互的过程。

HUAWEI

长庆油田绿色园区网项目

挑战：

1、长庆油田园区网横跨陕、甘、宁三地，并在银川和西安设置有互联网出口，伴随园区网内业务终端数量的不断增长，互联网带宽压力骤升；需要对互联网出口进行流量监控、协议分析，对P2P等异常流量进行管控，避免互联网出口带宽被滥用。

2、对数据中心（服务器群），生产指挥中心以及到中石油总部的敏感链路进行流量监控、协议分析，对恶意攻击流量进行过滤和清洗；保障关键业务资源的可用性和可服务性。

华为解决方案：

园区网部署业务监控网关（SIG9280E），利用分光设备或采用端口镜像的方式对西安、银川两地的互联网出口以及关键业务资源的访问链路进行流量镜像，对网络链路中的报文进行深度监控和检测，所有的异常流量经过华为万兆防火墙（USG9310）进行清洗、过滤后回注到业务环境中。

该解决方案采用旁路监测、深度报文分析、BGP策略路由等多种技术结合，安全、高效地为长庆油田创造了绿色园区网络空间。

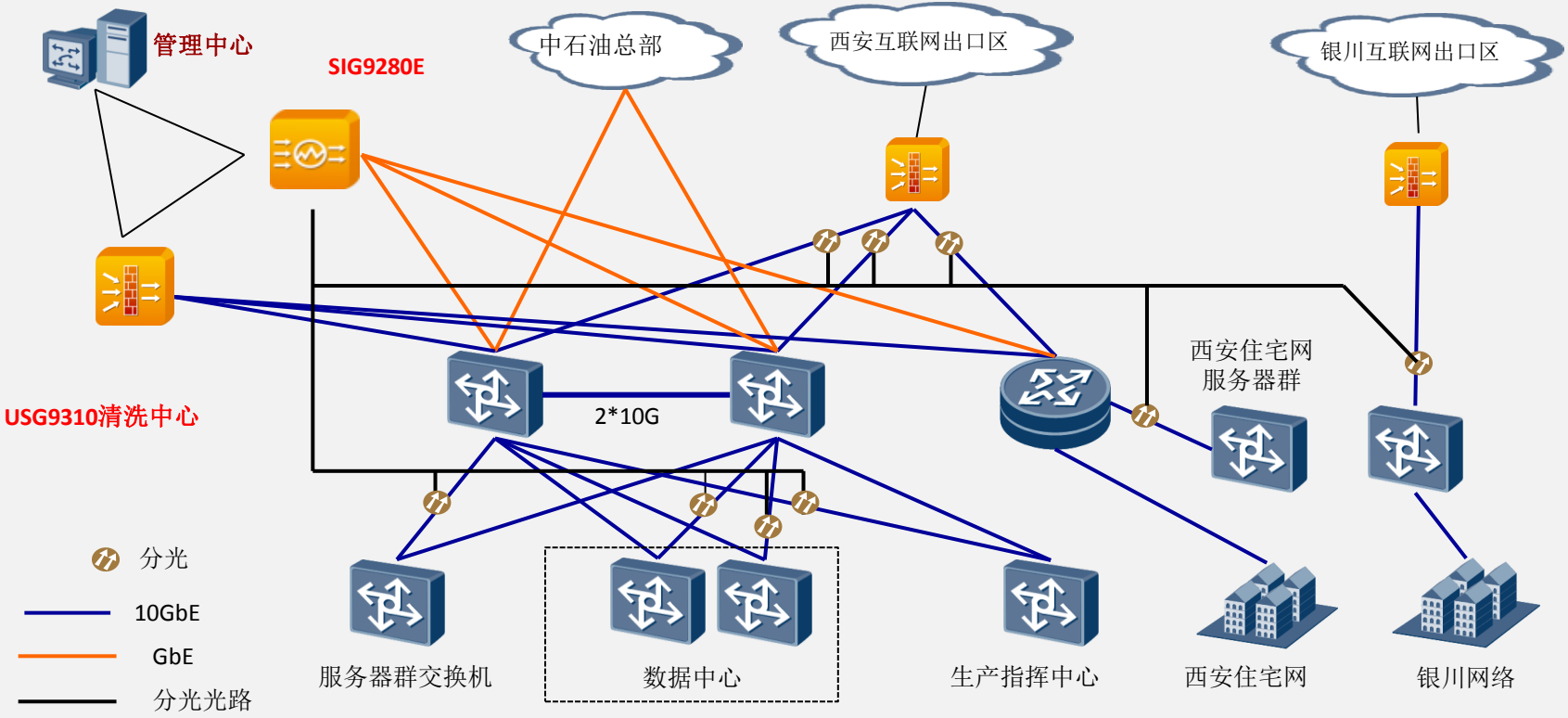
客户价值：

不更改现有网络拓朴结构，对企业园区网的互联网出口流量检测和管控，既保障互联网带宽的合理使用，又避免来自互联网的威胁攻击。

对企业内部的核心资源提供了网络级的整体防护，有效避免来自于园区网内部的攻击威胁。

中国石油长庆油田公司(PCOC)是隶属于中国石油天然气股份有限公司（PetroChina）的地区性油田公司，总部设在陕西省西安市，工作区域在中国第二大盆地－－鄂尔多斯盆地，横跨陕、甘、宁、内蒙古、晋五省（区），勘探总面积37万平方公里。

长庆油田绿色园区网解决方案



辽河油田勘探公司流量控制解决方案

中国石油天然气集团公司
CHINA NATIONAL PETROLEUM CORPORATION

挑战：

随着宽带接入的高速发展，辽河石油勘探局的内网ADSL用户、办公网员工数量及带宽都有很快的增长。

庞大的用户需求，在线音乐、在线游戏、网络电视（IPTV）、多媒体语音通信（VoIP）、即时通讯IM和其它多媒体IP 应用的普及，对IP网络的结构和容量都提出很高要求。

每年互联网出口带宽的扩容压力和投入成本巨大。

华为解决方案：

华为SIG流量控制解决方案采用旁路部署的方式管理用户现网接近10G带宽的流量，进行详细的流量分析、P2P的精准控制

对于VOIP和共享接入进行分析和管理，在客户互联网出口带宽有限的条件下，通过对所有上网用户带宽流量的精细化分析和控制，实现合理化运营的目的。

客户价值：

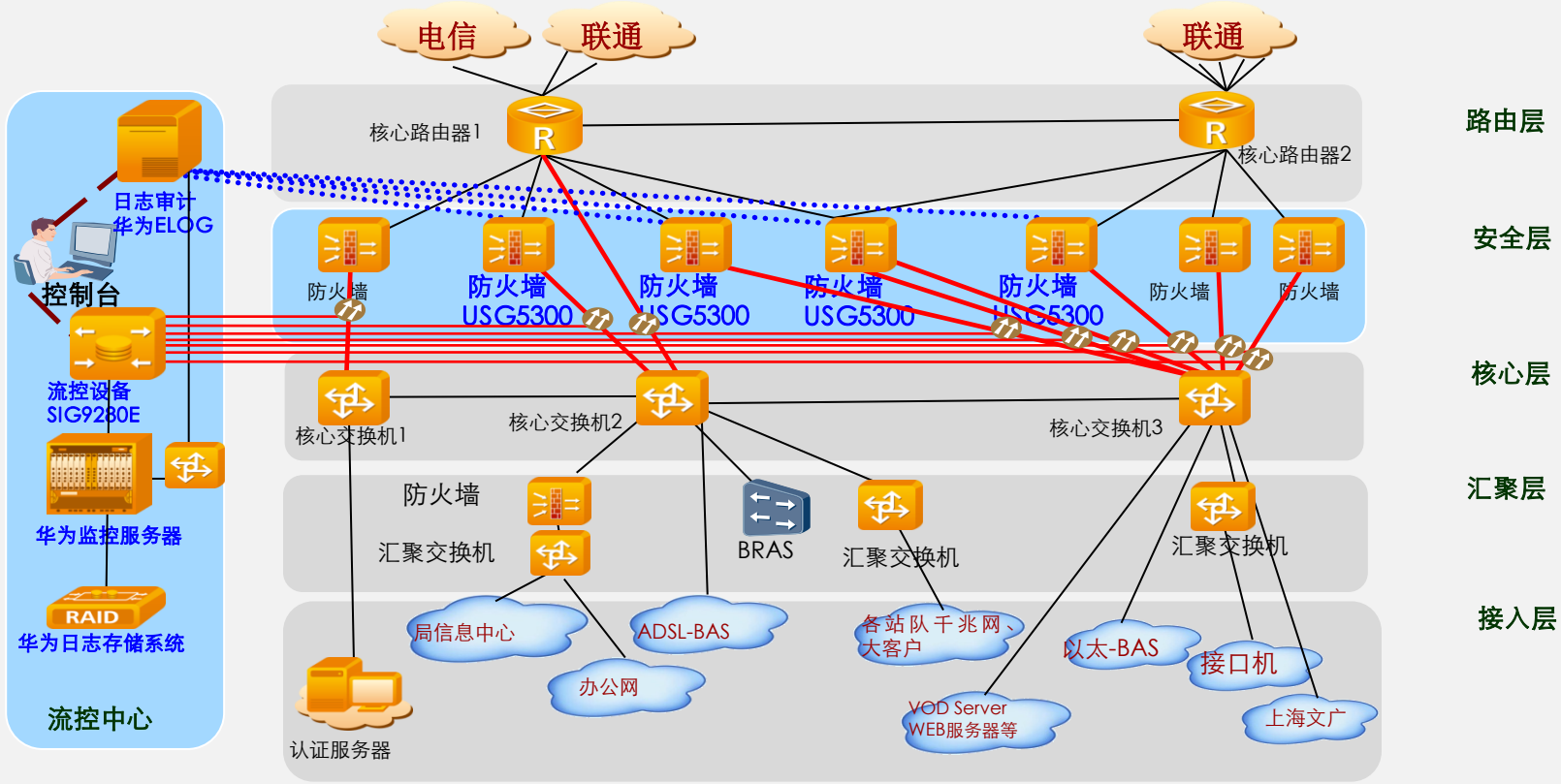
辽河油田宽带网络通过合理的流量分析和带宽控制，有效缓解用户集中上网时间段的大量P2P业务带来的带宽压力

同时通过精准的共享接入控制、VOIP控制进行精细化运营，在互联网出口带宽有限的前提下进行盈利性运营。

辽河石油勘探局是中国石油天然气集团公司所属骨干企业，总部坐落于美丽的新兴沿海开放城市辽宁省盘锦市。全局目前有47个二级单位，用工总量8万余人，资产总额197亿元。建成了中国第三大油田——辽河油田和全国最大的稠油、超稠油、高凝油生产基地。

HUAWEI

辽河油田勘探公司流量控制解决方案



HUAWEI

中海油总公司DDoS防护系统项目

挑战：

海油总公司互联网出口的抗DDoS系统已不能满足网络发展的需求，且已有设备无法形成对海油总部的网络防护，

总公司内部服务器受到DDoS攻击。对网络出口的DDoS防御以及网络带宽扩容对安全设备性能的提升是海油总公司亟待解决的问题。

华为解决方案：

网络出口部署高性能的USG9300高端电信级防火墙，配套业界领先的DDOS插板，对来自Internet的流量开启DDOS防护功能，实现千万包每秒的抗攻击能力，保证正常业务高效顺畅运行。

客户价值：

在不更改现有网络拓扑结构的情况下，对中海油总部的两条互联网出口进行了流量检测和清洗，

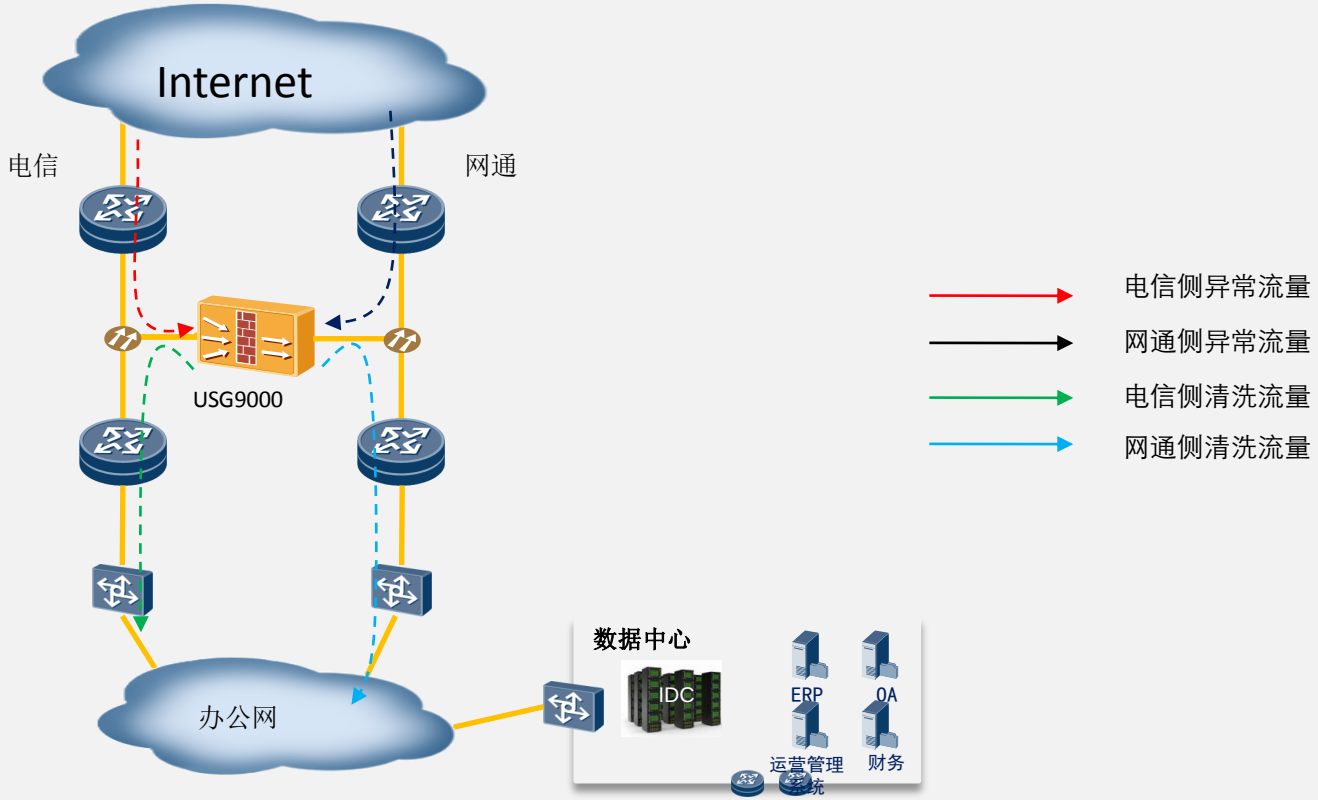
对DDoS异常流量攻击实施有效清洗，从而能够及时保证海油网络和业务的正常运行，同时满足未来互联网带宽扩容的需求。

中国海洋石油总公司
CHINA NATIONAL OFFSHORE OIL CORP.

中国海洋石油总公司（以下简称中国海油）是中国最大的国家石油公司之一，是中国最大的海上油气生产商。中国海油公司是一家主业突出、产业链完整的综合型能源集团，形成了上游、中下游、专业技术服务、金融服务以及新能源等产业板块。

HUAWEI

中海油总公司DDoS防护系统解决方案



HUAWEI

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY